

09642879-082100

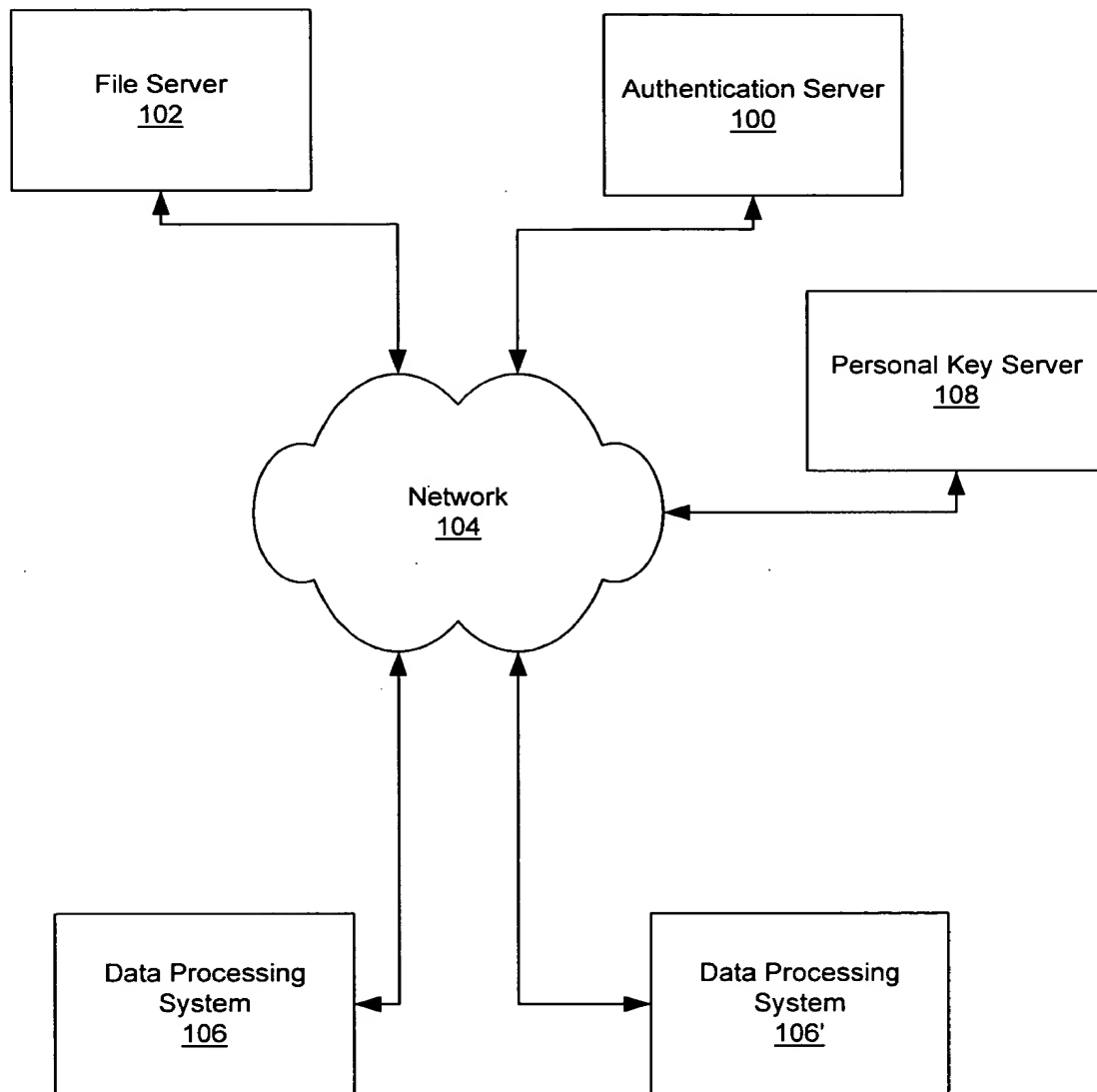


Figure 1

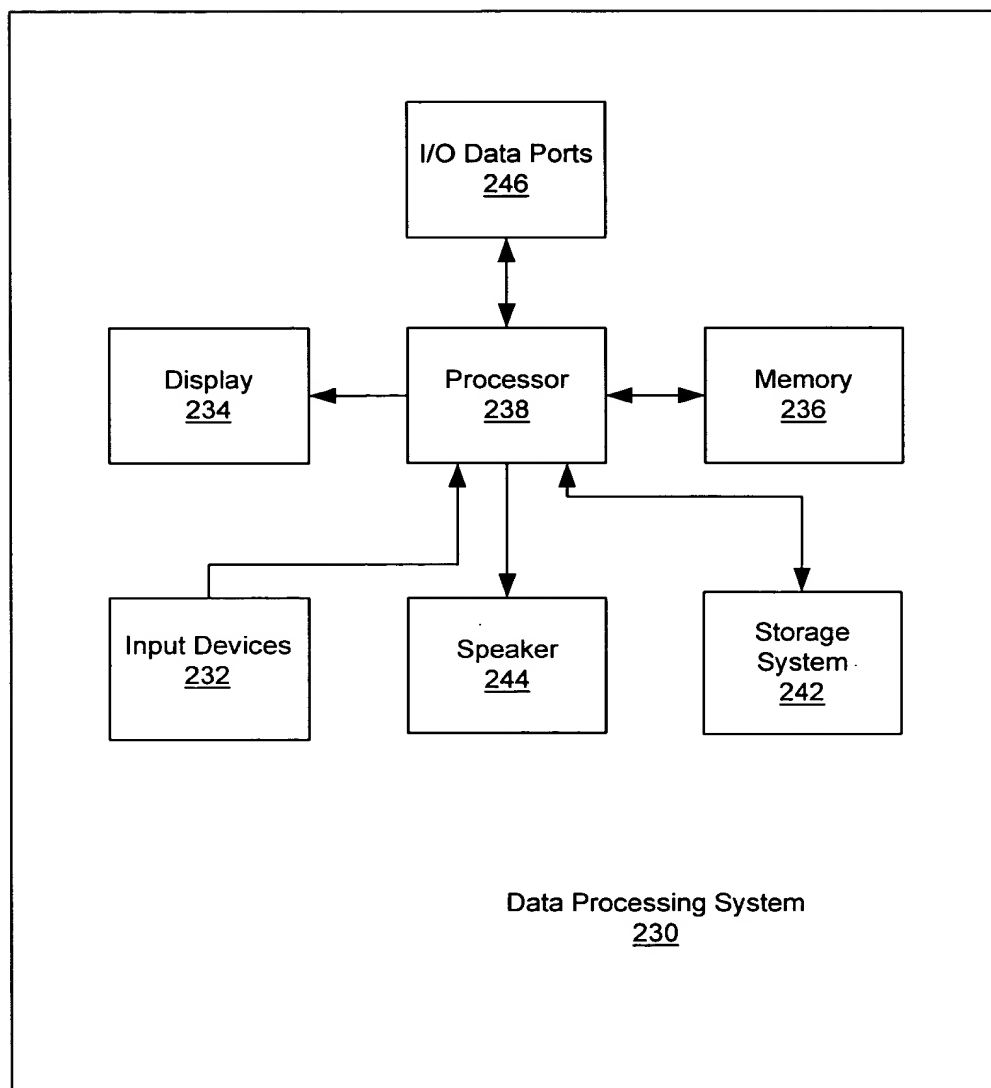


Figure 2

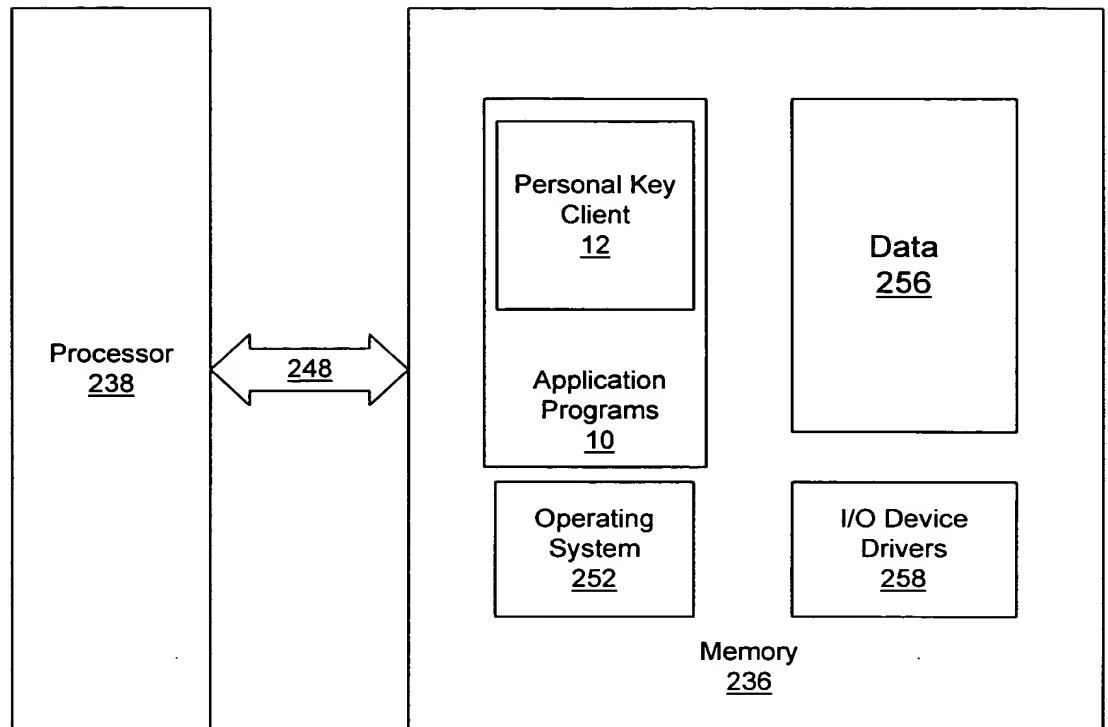


Figure 3

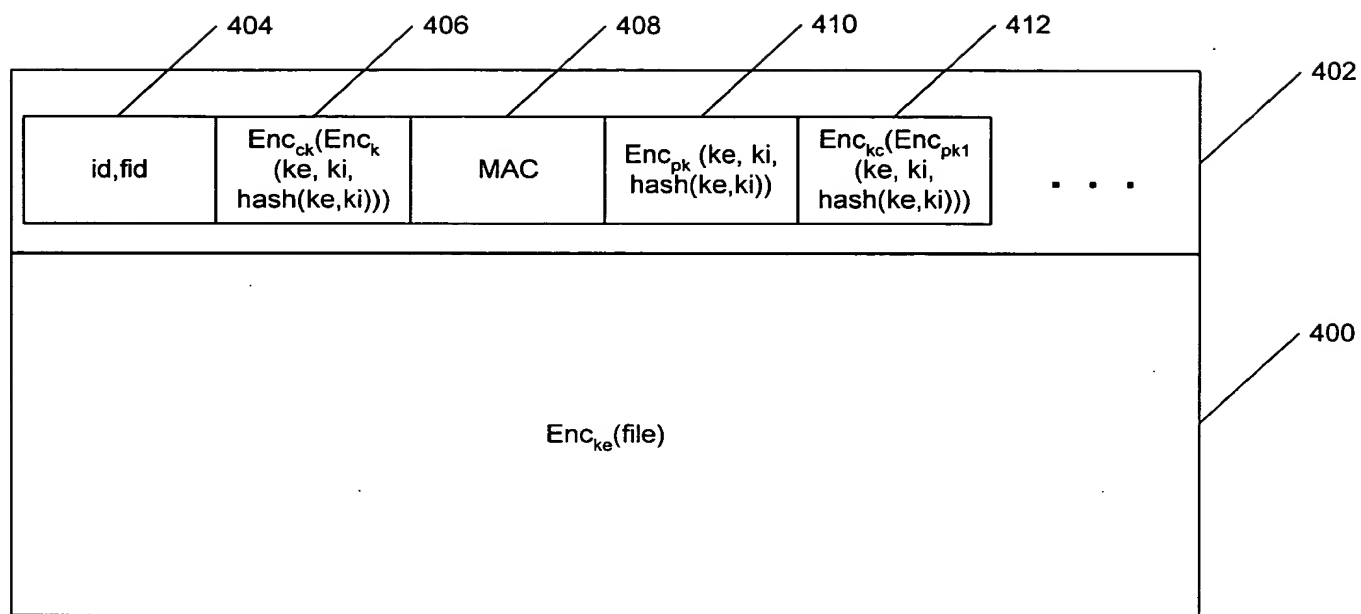


Figure 4

Figure 5

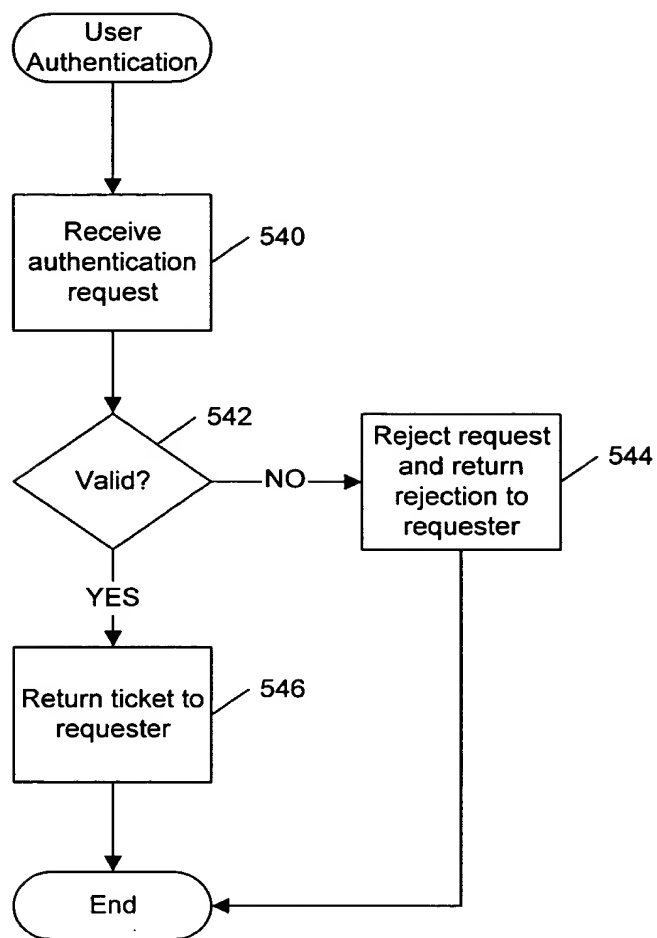
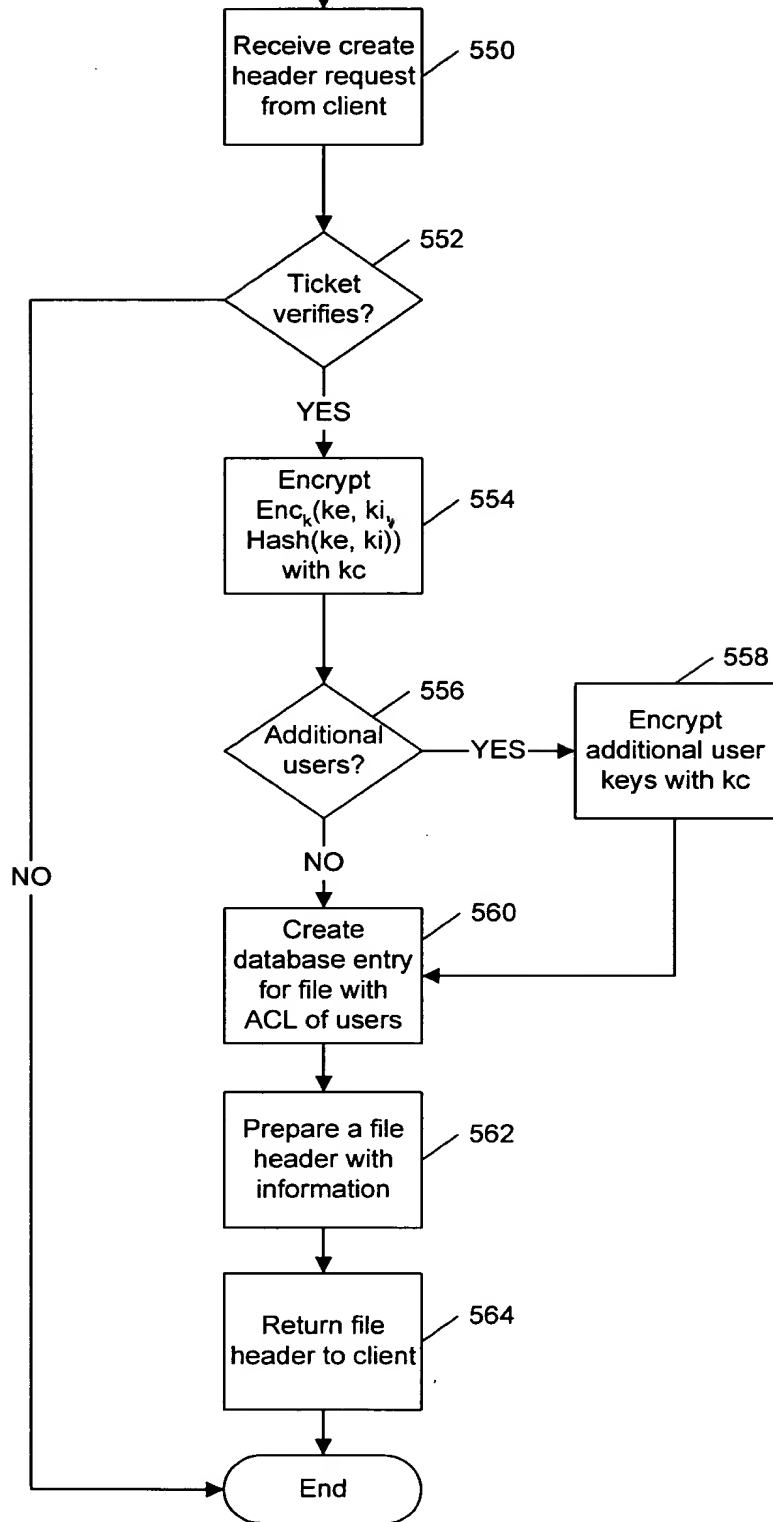


Figure 6

09642879.082100

Create Header



09642879.082.100

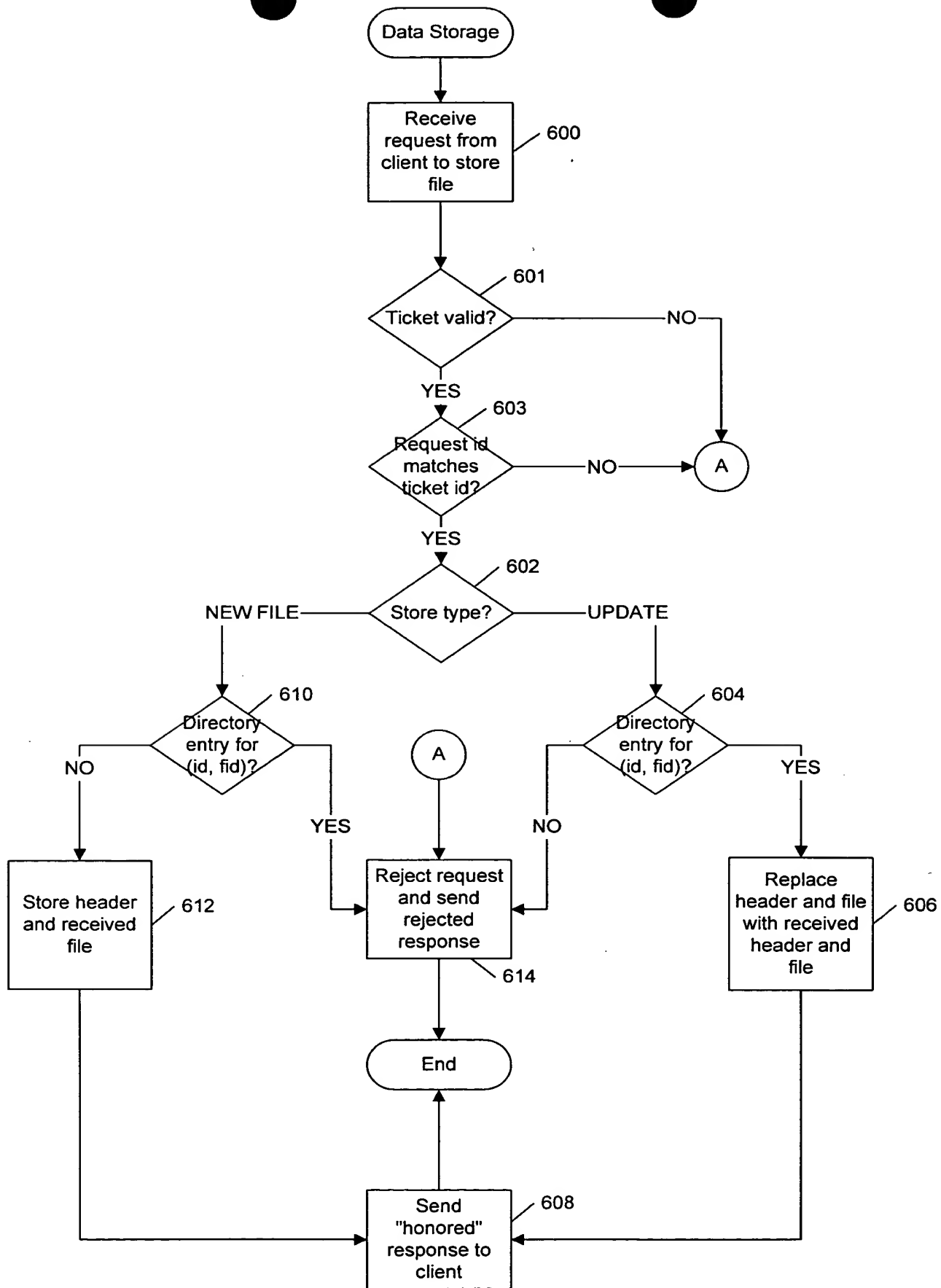


Figure 8

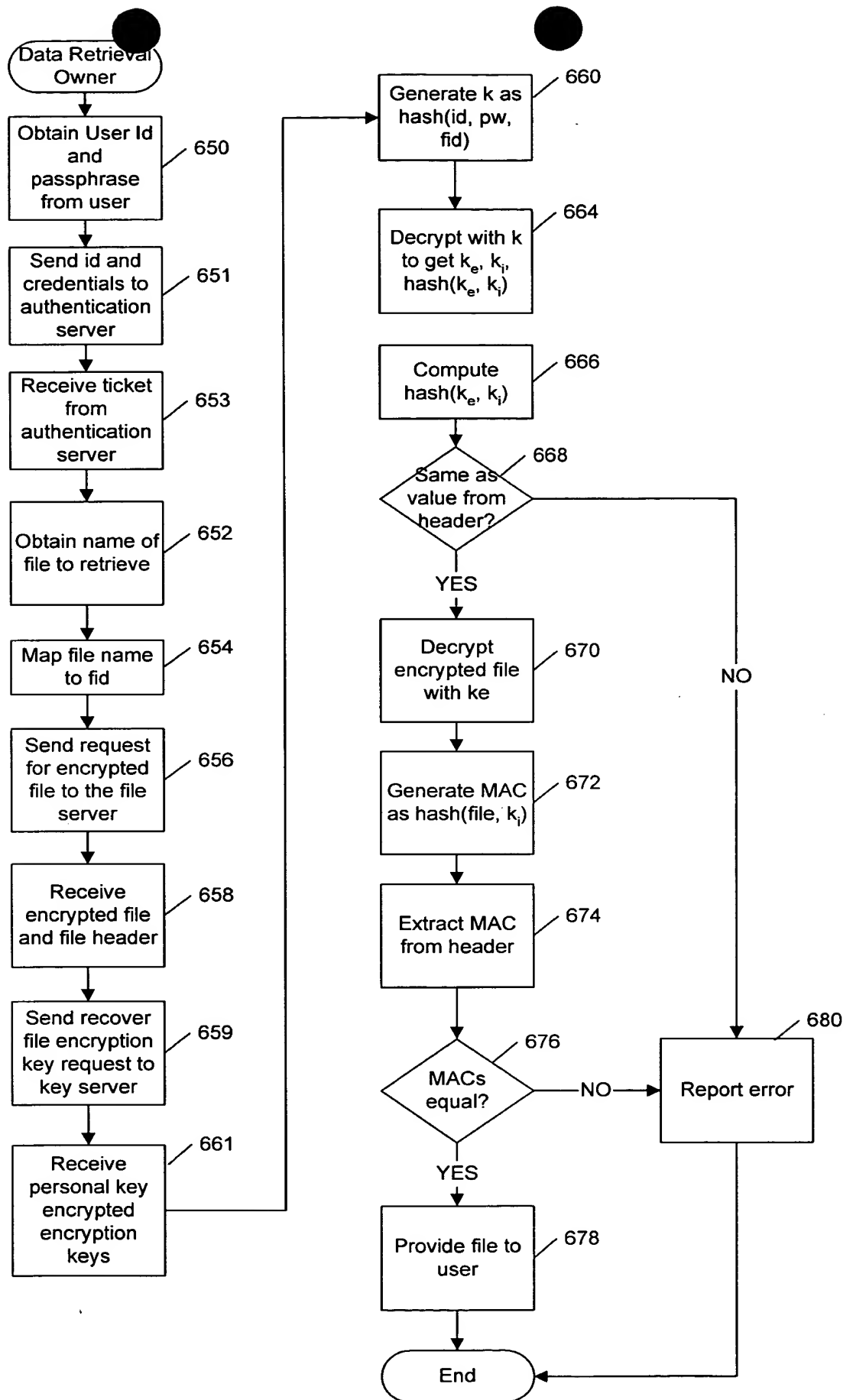


Figure 9

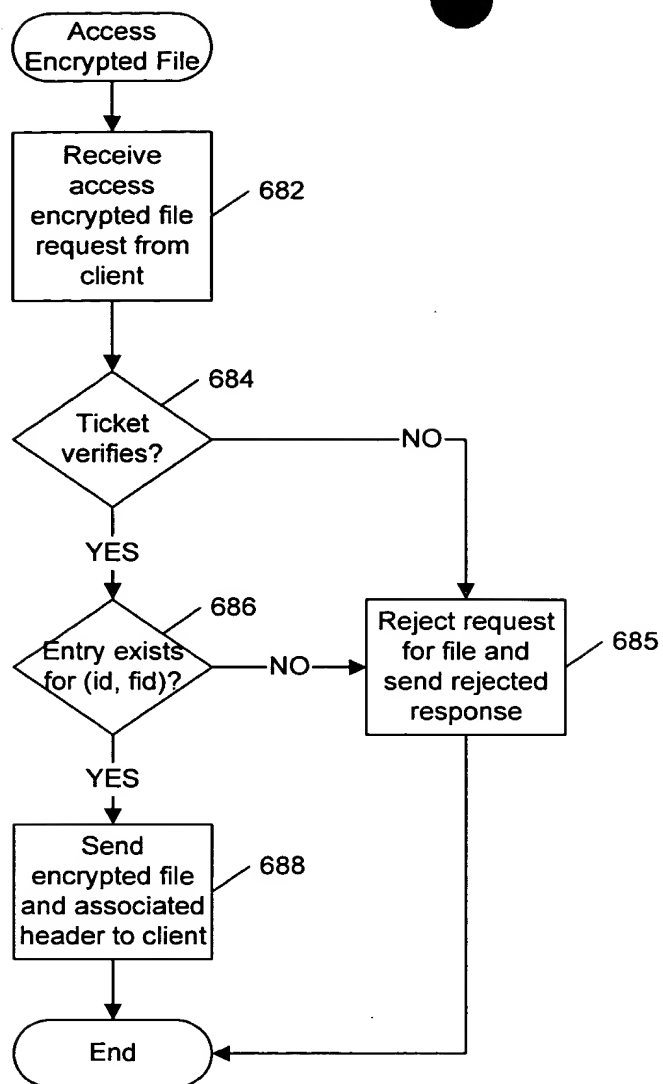


Figure 10

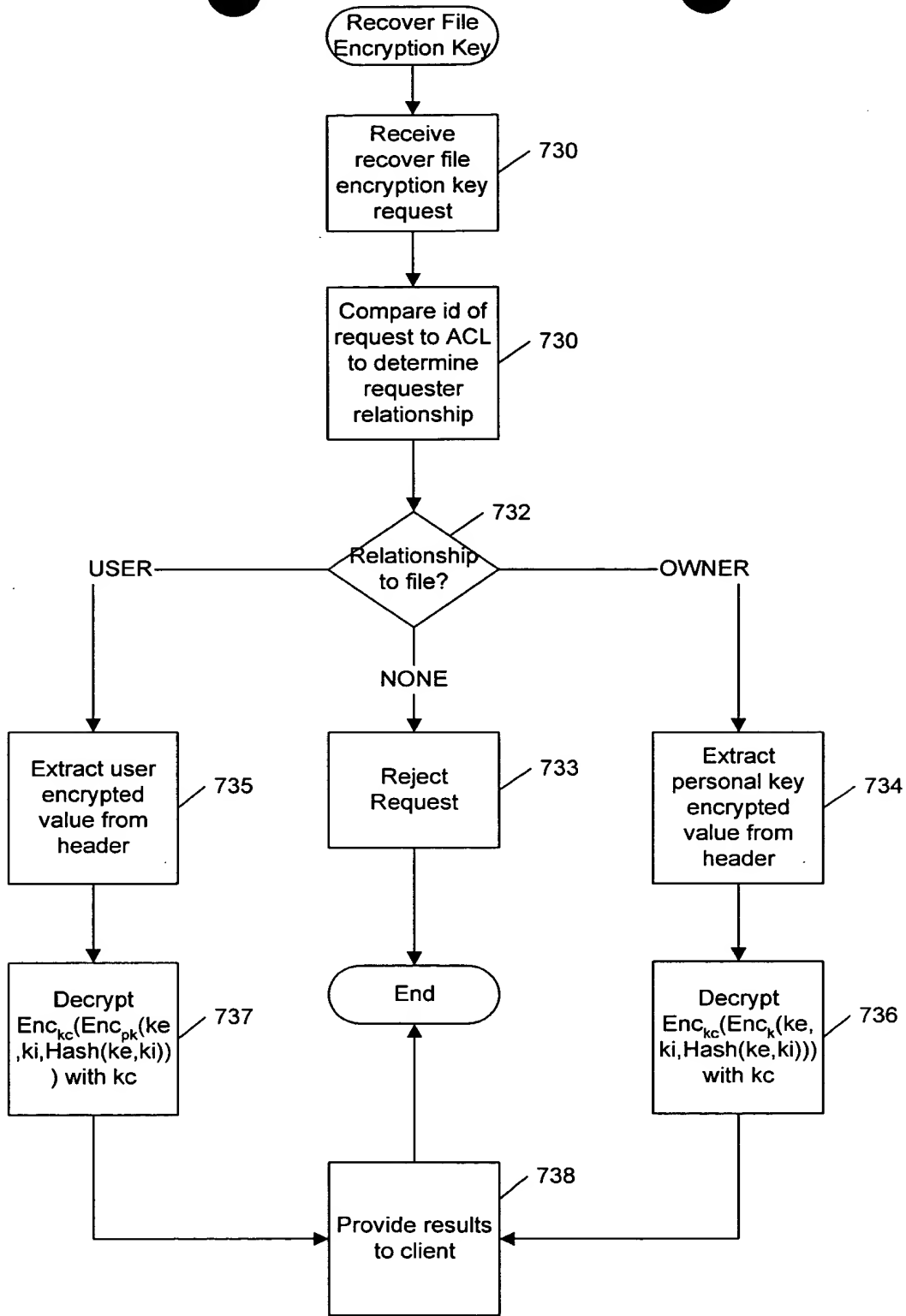


Figure 11

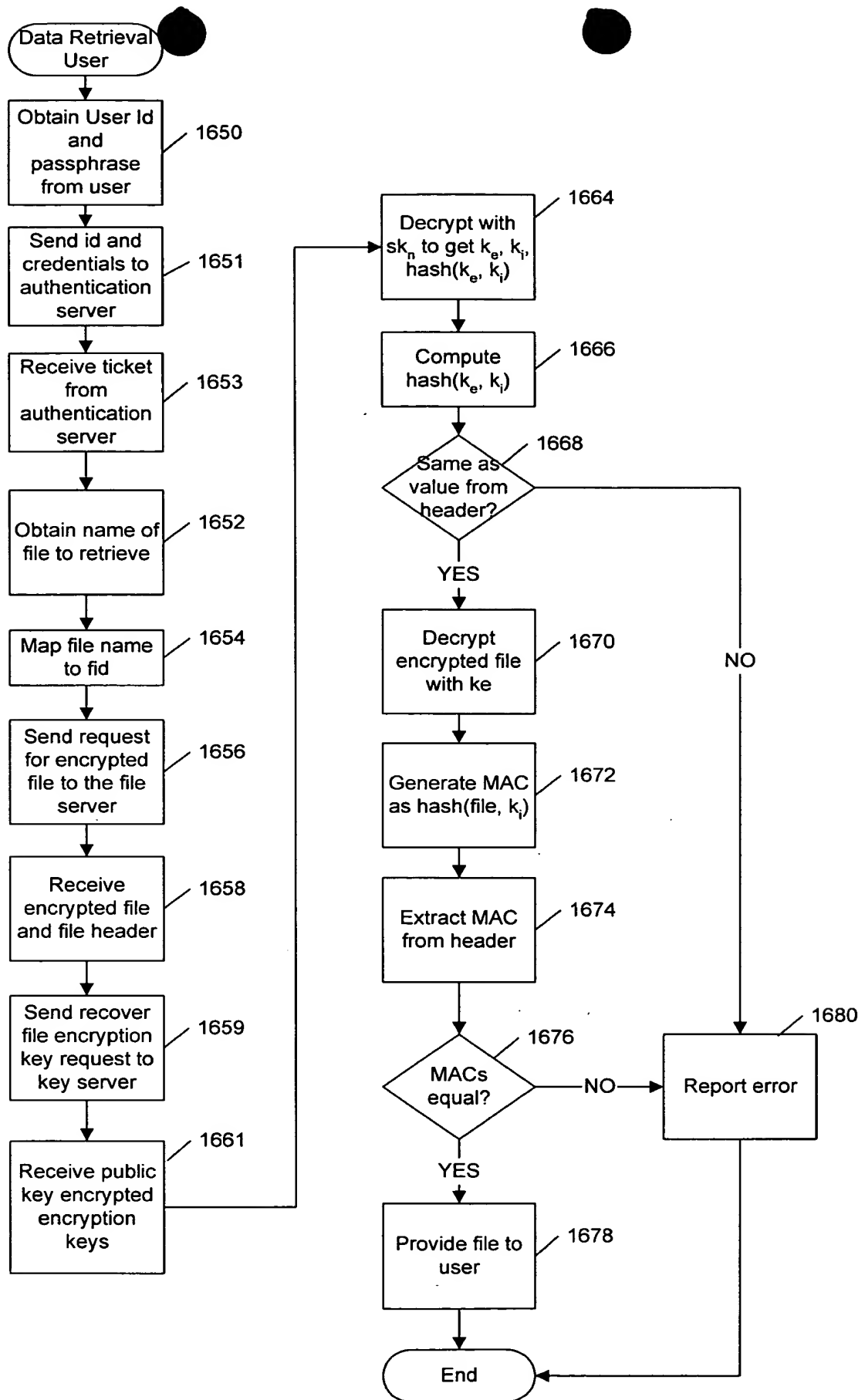


Figure 12

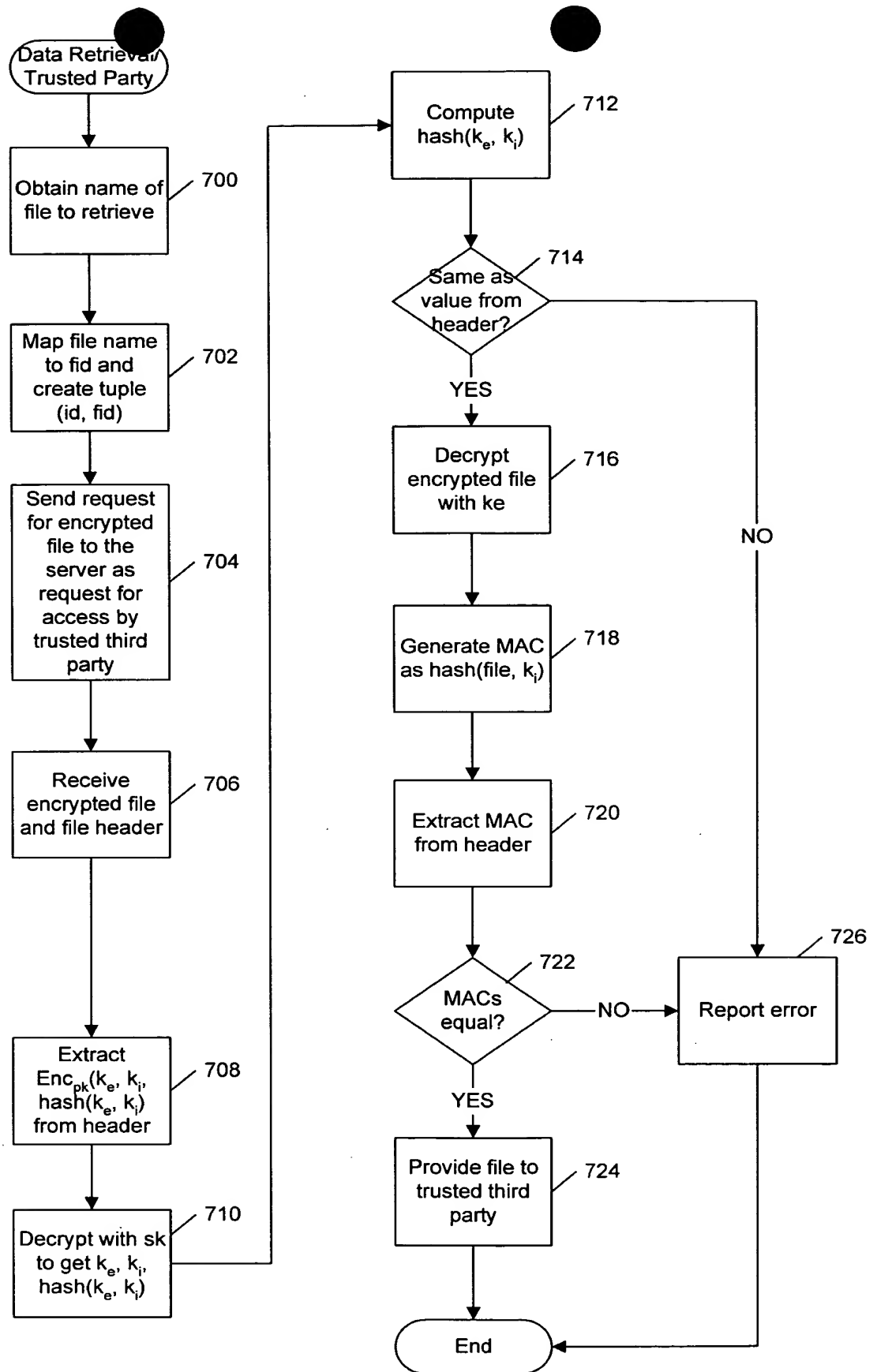


Figure 13

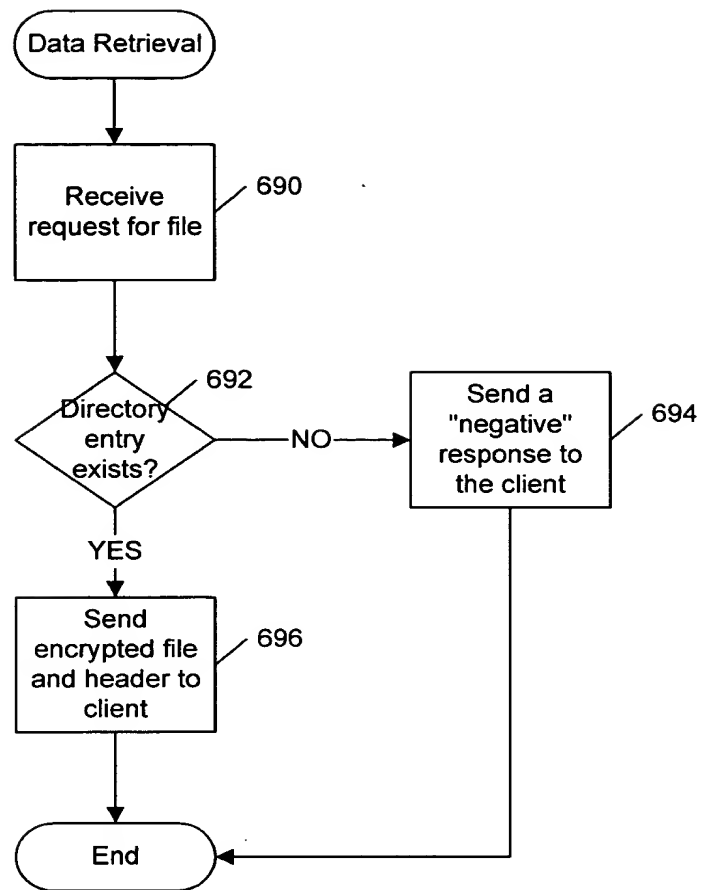
[illegible]

Figure 14

0321000

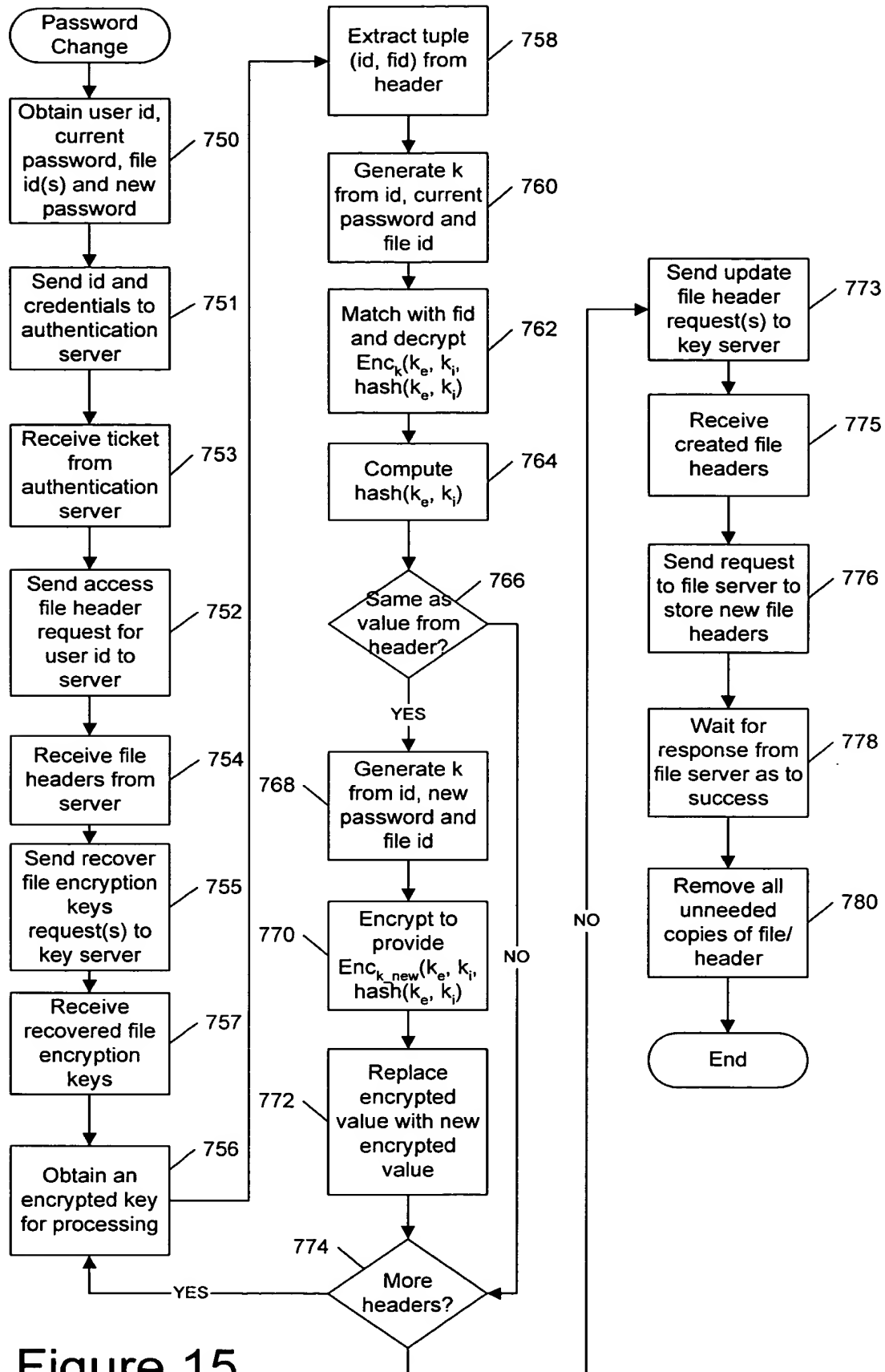
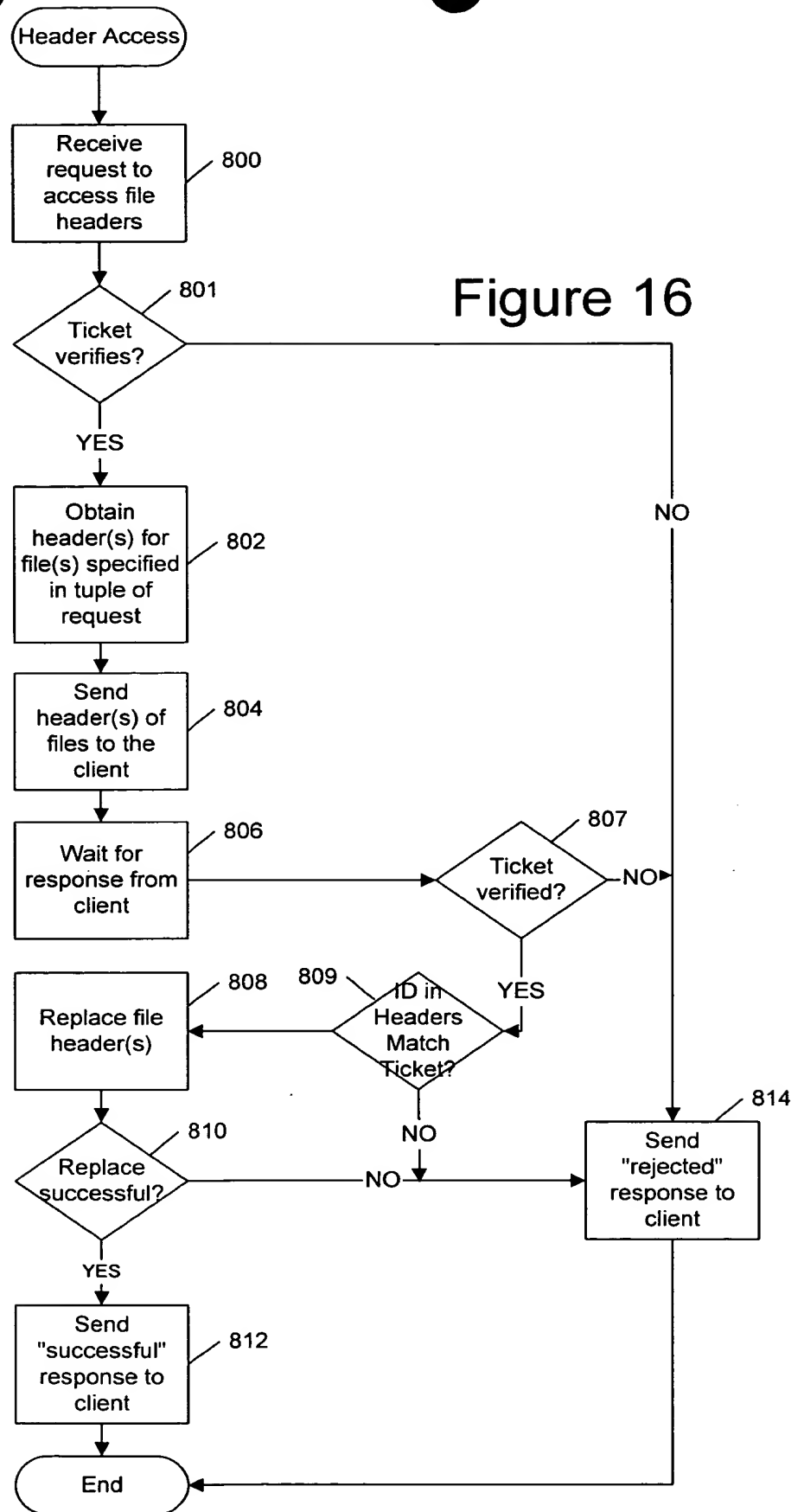


Figure 15

09642879 "082100



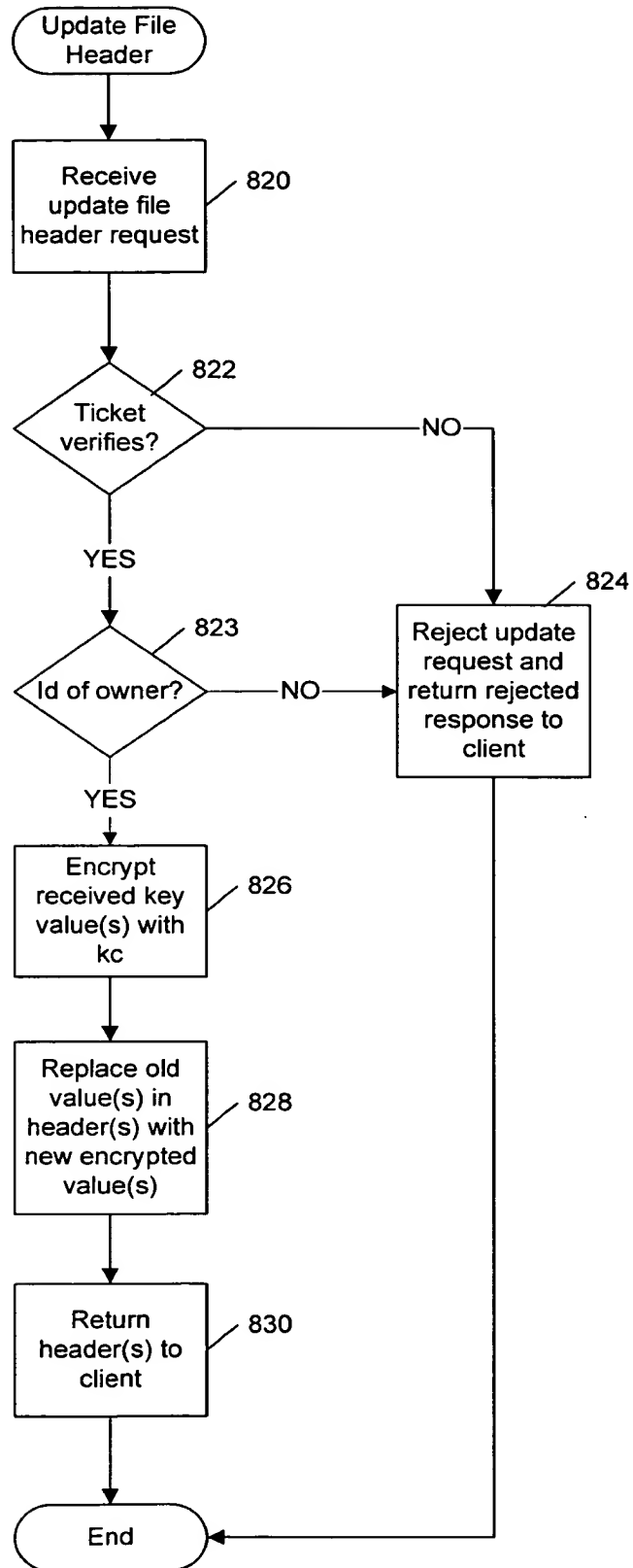


Figure 17

```

graph TD
    Start([Public Key Change]) --> 850[Obtain user id, current password, file id(s) and new public key]
    850 --> 851[Send id and credentials to authentication server]
    851 --> 853[Receive ticket from authentication server]
    853 --> 852[Send access file header request for user id to server]
    852 --> 854[Receive file headers from server]
    854 --> 855[Send recover file encryption keys request(s) to key server]
    855 --> 857[Receive recovered file encryption keys]
    857 --> 856[Obtain a file header for processing]
    856 --> 858[Extract tuple (id, fid) from header]
    858 --> 860[Generate k from id, current password and file id]
    860 --> 862[Match fid and decrypt  $Enc_k(k_e, k_i, hash(k_e, k_i))$ ]
    862 --> 864[Compute  $hash(k_e, k_i)$ ]
    864 --> 866{Same as value from header?}
    866 -- YES --> 868[Encrypt to provide  $Enc_{pk\_new}(k_e, k_i, hash(k_e, k_i))$ ]
    866 -- NO --> 872{More headers?}
    868 --> 870[Replace previous public key encrypted value with new encrypted value]
    870 --> 872
    872 -- YES --> 856
    872 -- NO --> 874[Send request to server to store new file headers]
    874 --> 876[Wait for response from server as to success]
    876 --> 878[Remove all unneeded copies of file/header]
    878 --> End([End])
  
```

Figure 18

Figure 18

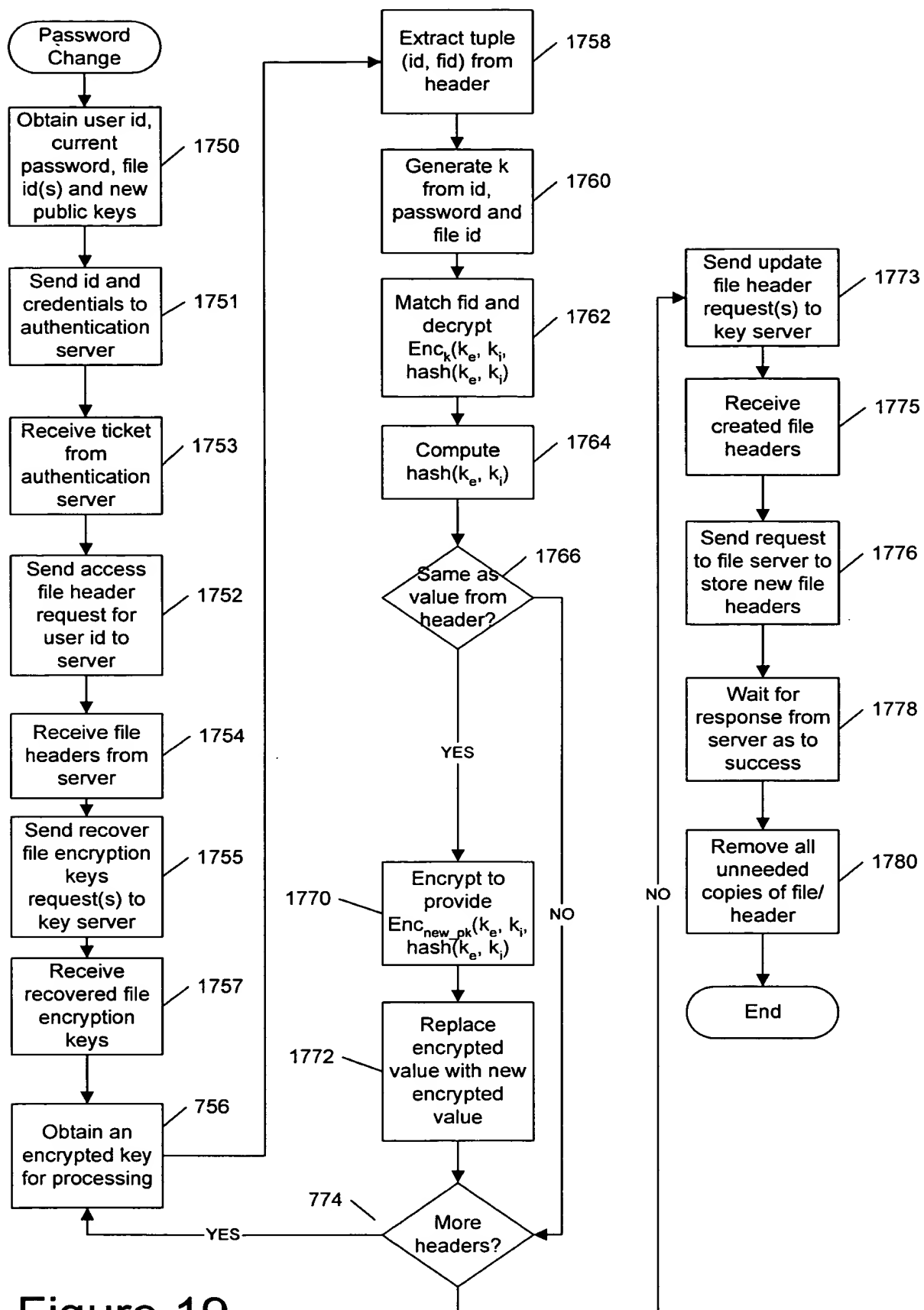


Figure 19